Desain *S-Box Fleksibel* Menggunakan LFSR Sebagai *Koefisien* Dan *Konstanta* Pada Fungsi *Linier*

[1)]Andre Pasopati Purba, [2)]Alz Danny Wowor, S.Si, M.Cs.
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email: [1)] 672013109@student.uksw.edu, [2)] alzdanny.wowor@uksw.edu

Abstract

Cryptography is often used for data protection due to many techniques it has. This research aims to scrutinize the comparison of s-box static and s-box flexible based on statistic examination. The result shows that s-box static has the least error score and the correlation is closer to zero compare to s-box flexible. Therefore, s-box static is proven to be more effective to use.

Keywords: *Cryptography, S-Box, Linear Function, LFSR, Design S-Box Flexible.*

Abstrak

Kriptografi sering digunakan dalam pengamanan data karena memiliki banyak teknik. Penelitian ini bertujuan untuk melihat desain dari penggunaan s-box fleksibel menggunakan LFSR sebagai koefisien dan konstanta pada fungsi linier berdasarkan pengujian statistic. Hasil penelitian ini menunjukkan bahwa desain s-box fleksibel memiliki nilai error yang paling kecil pada pengujian static banyak plainteks dan korelasi yang mendekati angka 0 (nol). Hasil ini menunjukkan bahwa desain s-box fleksibel menggunakan LFSR sebagai koefisien dan konstanta pada fungsi linier baik untuk dipergunakan.

Kata Kunci: *Kriptografi, S-Box, Fungsi Linear, LFSR, Desain S-Box Fleksibel.*

[1)] Mahasiswa Fakultas Teknologi Informasi Jurusan Teknik Informatika, Universitas Kristen Satya Wacana Salatiga.

[2)] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga.